



Weekly Wright Report (12/26/17)

GOVERNMENT CONTRACTING

As a Government Contractor, Will You Be Compliant by December 31st?

The clock is running out on the deadline for defense contractors to comply with the Department of Defense (DoD) mandate that requires contractors, and applicable subcontractors, to provide “adequate security” for covered defense information that is processed, stored, or transmitted on the contractor’s internal information system or network. The deadline for compliance is December 31, 2017.

By that date, all DoD contractors that process, store or transmit Controlled Unclassified Information (CUI) must comply with minimum security standards enumerated in the Defense Federal Acquisition Regulation Supplement (DFARS). DFARS clause 252.204-7012 expands safeguards to include cyber indecent reporting. Mandatory controls are detailed in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.”

Defense contractors should take note that DFARS 252.204-7012 requires contractors to report “cyber incidents” to the DoD within 72 hours of their discovery – so called “rapid reporting.” The definition of “cyber incident” includes actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. A “compromise” in turn means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred. Thus, a reporting requirement exists if someone copies covered defense information to unauthorized media, such as downloading covered information to a thumb drive or the cloud.

It is the contractor’s responsibility to determine whether it is has fully and properly implemented NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information). Third-party assessments or certifications of compliance are not required, authorized, or recognized by DoD, nor will DoD certify that a contractor is compliant with the NIST SP 800-171 security requirements. Ask Mike Stover mstover@wcslaw.com.



INSURANCE LAW

Is Your Company Subject to Fines Under the Affordable Care Act?

Employers of a significant size – generally 50 or more full-time employees – must provide full-time employees with health insurance that meets certain coverage minimums and is affordable. The Affordable Care Act (ACA) imposes penalties for failure to do so. So far, however, penalties have not yet been assessed, possibly because of the uncertainties about the existential future of the act. Employers have been hopeful that non-enforcement would continue. That, however, may be nearing an end with the announcement by the IRS that penalties will begin to be assessed.

Companies or employers who should be mindful are those having at least 50 full time employees during the preceding calendar year and, for at least one month of the year, had at least one full-time employee enrolled in a qualified health plan for which a health insurance marketplace subsidy was issued. The IRS may seek a penalty if the employer does not meet the standards to take advantage of the affordability safe harbor or other appropriate relief.

The IRS may issue a document called **Letter 226J**. The letter explains the penalty and contains a table describing the monthly payment. It also contains a response form for the employer to file, and a document that shows, by month, the employer's full-time employees who received the subsidy and had not been offered employer coverage.

In addition, the letter will include instructions to the employer for what to do if it either agrees or disagrees with the proposed payment, and finally a warning of consequences for failure to respond within 30 days from the date of the letter. Should the employer file an answer disagreeing with the penalty, the employer can request a conference with the IRS Office of Appeals. If the employer does not respond, the penalty will be assessed as proposed and payment will be demanded.

Employers should be on the lookout for IRS **Letter 226J** and pay close attention to its requirements and deadlines. Ask Jim jconstable@wcsllaw.com

EMPLOYMENT LAW

#MeToo is Time Magazine's Person of the Year

Having created a wave of awareness about sexual harassment and assault, taking down many powerful men in the process, the #MeToo movement has been named *Time* magazine's Person of the Year for 2017. The article features women and men who have spoken out, including activist Tarana Burke, who started the hashtag 10 years ago. Learn how to protect your workplace. Contact Laura LRubenstein@wcsllaw.com